

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-297551
 (43)Date of publication of application : 11.10.2002

(51)Int.Cl. G06F 15/00
 G06K 17/00
 G06K 19/00
 H04L 9/32

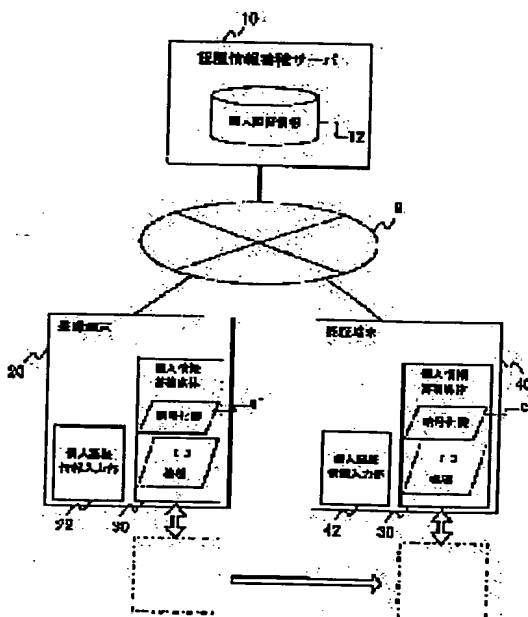
(21)Application number : 2001-101906 (71)Applicant : MITSUBISHI ELECTRIC CORP
 (22)Date of filing : 30.03.2001 (72)Inventor : OKUDA HARUHISA
 HIRAI TAKAHIDE
 SHIKAI MASAHIRO
 SHIROTSUKI AKIHIDE
 OKA TORU
 TATSUBO HIROKAZU
 TSUTADA HIROYUKI

(54) IDENTIFICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain an identification system which safely and surely performs user identification even between different terminals.

SOLUTION: Biometrics information such as fingerprints, irises and handwriting of a user is encoded by using a registration terminal 20 beforehand and registered in an identification information storage server 10. Also, key information for use in encoding and decoding it, registration terminal model information and user identification information are recorded in a portable personal information storage medium 30. When receiving identification in an identification terminal 40, encoded biometrics information acquired from the above identification information storage server 10 is decoded by using the encoding key e1 of the personal information storage medium 30. The user identification is performed by collating the decoded biometrics information with the reentered biometrics information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-297551
(P2002-297551A)

(43) 公開日 平成14年10月11日 (2002. 10. 11)

(51) Int.Cl.	識別記号	F I	テ-リ-ト* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 3 5
G 0 6 K 17/00		G 0 6 K 17/00	V 5 B 0 5 8
19/00		19/00	Q 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D 5 J 1 0 4
			6 7 5 A

審査請求 未請求 請求項の数 5 O L (全 21 頁) 最終頁に続く

(21) 出願番号 特願2001-101906(P2001-101906)

(22) 出願日 平成13年3月30日 (2001. 3. 30)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 奥田 晴久

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72) 発明者 平井 敬秀

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

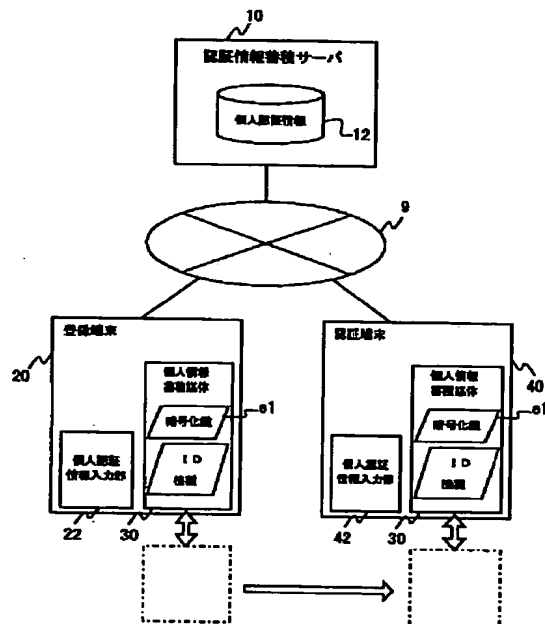
最終頁に続く

(54) 【発明の名称】 認証システム

(57) 【要約】

【課題】 ユーザ認証を、異なる端末間においても安全かつ確実に起こう認証システムを得ること。

【解決手段】 あらかじめ登録端末20を用いてユーザの指紋、虹彩、筆跡等のバイオメトリクス情報を暗号化して認証情報蓄積サーバ10に登録するとともにその暗号化および復号化のための鍵情報、登録端末機種情報、ユーザID情報を搬送可能な個人情報蓄積媒体30に登録しておき、認証端末40において認証を受ける際に、上記した認証情報蓄積サーバ10から取得した暗号済みのバイオメトリクス情報をその個人情報蓄積媒体30の暗号化鍵e1を用いて復号し、復号化したバイオメトリクス情報と、改めて入力したバイオメトリクス情報とを照合することでユーザの認証をおこなう。



【特許請求の範囲】

【請求項1】 少なくとも暗号化鍵を記録した個人情報蓄積媒体と、
ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、
を備え、
前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする認証システム。

【請求項2】 少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、
ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、
電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受

信するアプリケーションサーバと、

を備え、
前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする認証システム。

【請求項3】 少なくとも暗号化鍵を記録した個人情報蓄積媒体と、
ユーザの第1のバイオメトリクス情報を入力し、入力した第1のバイオメトリクス情報を複数の第2のバイオメトリクス情報に分割し、各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第2のバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの第2のバイオメトリクス情報を蓄積し、蓄積した第2のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第2のバイオメトリクス情報を併合して前記第1のバイオメトリクス情報を復元し、復元した第1のバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、
を備え、
前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする認証システム。

【請求項4】 少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、
ユーザの第1のバイオメトリクス情報を入力し、入力した第1のバイオメトリクス情報を複数の第2のバイオメトリクス情報に分割し、各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第2のバイオメトリクス情報を送信する登録端末と、
前記登録端末から送信された暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの第2のバイオメトリクス情報を蓄積し、蓄積した第2のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、
ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第2のバイオメトリクス情報を併合して前記第1の

バイオメトリクス情報を復元し、復元した第1のバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、

電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、
を備え、

前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする認証システム。

【請求項5】 前記認証情報蓄積サーバが蓄積したバイオメトリクス情報と同一内容のバイオメトリクス情報を蓄積した複数のミラーサーバを備え、

前記登録端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つに対して、前記暗号化したバイオメトリクス情報を送信し、

前記認証端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つから、前記暗号化したバイオメトリクス情報を受信することを特徴とする請求項1～4のいずれか一つに記載の認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、通信回線を介してサービスを受信する際のユーザ認証をおこなう認証システムに関し、特に、そのユーザ認証を、異なる端末間においても安全かつ確実におこなうことができる認証システムに関するものである。

【0002】

【従来の技術】近年において急速に広まったインターネットは、オープンなネットワークであるがゆえに、自分が送信したデータが第三者に盗み見される可能性を否定できないという問題を有している。そこで、暗号化技術を導入することで、WebサーバとWebブラウザとの間でクレジット・カード番号などを安全に送信したり、メールの送信者や内容が偽造されたりしていないことを証明するといったデータの保安性が図られている。

【0003】ここで、インターネット上の暗号化技術の代表的なものとしては、共通鍵暗号法と公開鍵暗号法が知られている。共通鍵暗号法は、自分と相手と同じ暗号鍵を使って暗号化と復号化をおこなう方法である。一

方、公開鍵暗号法は、現在主流となっている暗号方法であり、秘密鍵と公開鍵という二つの鍵ペアを用いて暗号化と復号化をおこない、どちらか一方の鍵で暗号化したデータは、もう一方の鍵を使わないと復号化できないという特徴を有している。

【0004】この公開鍵暗号法において、秘密鍵は、その名の通り、所持者（使用権限のある者）だけが自由に使うことができるため、自身で安全に管理しなければいけない。また、公開鍵は、インターネット上等で広く公開されており、誰でも取得して利用できるようにされている。ここで、秘密鍵を使って暗号化することは、復号化するための公開鍵を誰もが入手できるので一見意味がないように思えるが、実はそうではなく、秘密鍵を使ってデータを暗号化すれば、そのデータをペアとなる公開鍵で復号化することにより、確かにそのデータが秘密鍵保持者によって暗号化されたことを確認できるという利点を有している。すなわち、これにより本人性を確認することができ、この性質を利用したものが、いわゆるデジタル署名である。

【0005】デジタル署名は、送信者（作成者）を特定するために、電子的に作成された文書（メッセージ）に添付され、電子商取引や電子申請をサポートする電子認証システムにおいて、非常に重要な役割を果たしている。具体的には、送信者により作成されたメッセージからハッシュ値を抽出することでメッセージの縮小版であるメッセージダイジェストを作成し、つづいてこのメッセージダイジェストを送信者自身の秘密鍵で暗号化することにより作成される。

【0006】デジタル署名を利用した認証システムは、認証書保持者（メッセージ送信者）、認証書依拠者（メッセージ受信者）および認証局（公開鍵認証書発行者）の三者により構成されるのが一般的である。ここで、公開鍵認証書とは、メッセージ送信者が誰であるかを確認できるものであり、通常、認証を受けたメッセージ送信者の公開鍵とそのメッセージ送信者に関する情報（属性）とが含まれている。また、公開鍵認証書は認証局から発行され、発行を受けた本人のみが、その認証書に対応する秘密鍵を使用することができる。さらに、公開鍵認証書には、発行元の認証局を明らかにするために、認証局のデジタル署名がされている。よって、認証局は、強い公共性を持った場合が多い。

【0007】一方、ユーザ認証をおこなう方法の一つとして、バイオメトリクス認証が注目されている。バイオメトリクス認証とは、指紋、虹彩、掌紋、音声、筆跡などの個人に固有の生体情報に基づいて、ユーザを特定する方法である。よって、バイオメトリクス情報の入力に際しては、本人以外がそれを実行することは不可能であり、より安全性の高いユーザ認証が可能となる。

【0008】このようなバイオメトリクス情報をユーザ認証に利用した認証システムとしては、例えば特開20

00-092046号に「遠隔認証システム」が開示されている。この「遠隔認証システム」によれば、ユーザの個人情報であるバイオメトリクス情報を暗号化し、バイオメトリクス情報をユーザが指定した認証サーバにのみ復号可能な状態でネットワークを転送するので、バイオメトリクス情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できる。

【0009】

【発明が解決しようとする課題】しかしながら、上記したデジタル署名によるユーザ認証では、一度、コンピュータ等の利用端末にデジタル署名を登録した後は、ユーザ認証時においてパスワードの入力が必要になるのみで、他人にパスワードが知られた場合に、その利用端末からのなりすましを防ぐことはできなかった。すなわち、ユーザ本人とデジタル署名との関連付けは、認証局等からデジタル署名を取得する際に必要となるだけであり、パスワードの漏洩といったソーシャルハッキングに対抗できるものではなかった。

【0010】一方、上記した特開2000-092046号に開示の「遠隔認証システム」では、認証サーバ側でバイオメトリクス情報を復号できたため、サーバ側で悪意を持ったオペレーションがおこなわれた場合、情報を完全に保護することができないという問題があった。

【0011】また、照合対象となるバイオメトリクス情報、すなわち登録されたバイオメトリクス情報を、携帯可能な記録媒体に記録することも可能であるが、一般にバイオメトリクス情報のサイズは、デジタル署名等に比較して非常に大きく、大容量の記録媒体を必要とするため、現実的ではない。さらに、その記録媒体が盗難にあった場合には、バイオメトリクス情報を解析して、なりすましも可能となる可能性が高い。

【0012】この発明は上記問題点を解決するためになされたもので、ユーザ認証を、異なる端末間においても安全かつ確実におこなう認証システムを得ることを目的とする。

【0013】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、この発明にかかる認証システムにあっては、少なくとも暗号化鍵を記録した個人情報蓄積媒体と、ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人

情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、を備え、前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする。

【0014】この発明によれば、あらかじめ登録したバイオメトリクス情報を、外部に位置する認証情報蓄積サーバが管理するので、認証端末のように、ユーザが登録時に使用した登録端末とは異なる端末を利用しようとする場合でも、個人情報蓄積媒体を移すことのみで、暗号化をともなった個人認証を実行することが可能となる。

【0015】つぎの発明にかかる認証システムにあっては、少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、ユーザのバイオメトリクス情報を入力し、入力したバイオメトリクス情報を、前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化したバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を蓄積し、蓄積したバイオメトリクス情報を要求に応じて送信する認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記認証情報蓄積サーバから前記暗号化済みのバイオメトリクス情報を受信し、受信した暗号化済みのバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化したバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、を備え、前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする。

【0016】この発明によれば、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、アプリケーションサーバ側が要求するユーザ認証を可能にする。

【0017】つぎの発明にかかる認証システムにあっては、少なくとも暗号化鍵を記録した個人情報蓄積媒体

と、ユーザの第1のバイオメトリクス情報を入力し、入力した第1のバイオメトリクス情報を複数の第2のバイオメトリクス情報に分割し、各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第2のバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの第2のバイオメトリクス情報を蓄積し、蓄積した第2のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第2のバイオメトリクス情報を併合して前記第1のバイオメトリクス情報を復元し、復元した第1のバイオメトリクス情報と入力したバイオメトリクス情報とを照合する認証端末と、を備え、前記登録端末、前記認証情報蓄積サーバおよび前記認証端末は通信回線を介して接続されたことを特徴とする。

【0018】この発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはこれらのサーバからの情報を併合するので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなる。

【0019】つぎの発明にかかる認証システムにあっては、少なくとも暗号化鍵および秘密鍵を記録した個人情報蓄積媒体と、ユーザの第1のバイオメトリクス情報を入力し、入力した第1のバイオメトリクス情報を複数の第2のバイオメトリクス情報に分割し、各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて暗号化し、暗号化した各第2のバイオメトリクス情報を送信する登録端末と、前記登録端末から送信された暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの第2のバイオメトリクス情報を蓄積し、蓄積した第2のバイオメトリクス情報を要求に応じて送信する複数の認証情報蓄積サーバと、ユーザのバイオメトリクス情報を入力するとともに、前記複数の認証情報蓄積サーバから前記暗号化済みの第2のバイオメトリクス情報を受信し、受信した暗号化済みの各第2のバイオメトリクス情報を前記個人情報蓄積媒体から読み込んだ暗号化鍵を用いて復号化し、復号化した各第2のバイオメトリクス情報を併合して前記第1のバイオメトリクス情報を復元し、復元した第1のバイオメトリクス情報と入力したバイオメトリクス情報とを照合して照合結果を出力し、前記秘密鍵と対になる公開鍵で暗号化されたセッションキーを受信し、受信した暗号化済みのセッションキーを前記個人情報蓄積媒体から読み込んだ秘密鍵を用いて復号化し、復号化したセッ

ションキーと前記照合結果とを前記秘密鍵で暗号化し、暗号化したセッションキーと照合結果を送信する認証端末と、電子商取引等のサービスを提供するとともに、前記秘密鍵と対になる公開鍵を取得し、前記認証端末に対してユーザ認証を要求する際に、セッションキーを生成し、生成したセッションキーを前記公開鍵で暗号化し、暗号化したセッションキーを前記認証端末に送信し、前記暗号化したセッションキーと照合結果を前記認証端末から受信するアプリケーションサーバと、を備え、前記登録端末、前記認証情報蓄積サーバ、前記認証端末および前記アプリケーションサーバは通信回線を介して接続されたことを特徴とする。

【0020】この発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはこれらのサーバからの情報を併合するとともに、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなり、また、アプリケーションサーバ側が要求するユーザ認証を可能にする。

【0021】つぎの発明にかかる認証システムにあっては、上記発明において、前記認証情報蓄積サーバが蓄積したバイオメトリクス情報と同一内容のバイオメトリクス情報を蓄積した複数のミラーサーバを備え、前記登録端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つに対して、前記暗号化したバイオメトリクス情報を送信し、前記認証端末は、前記認証情報蓄積サーバまたは前記複数のミラーサーバのいずれか一つから、前記暗号化したバイオメトリクス情報を受信することを特徴とする。

【0022】この発明によれば、複数の認証情報蓄積サーバにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができる。

【0023】

【発明の実施の形態】以下に、この発明にかかる認証システムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【0024】実施の形態1。まず、実施の形態1にかかる認証システムについて説明する。実施の形態1にかかる認証システムは、あらかじめ登録端末を用いてユーザの指紋、虹彩、筆跡等のバイオメトリクス情報を暗号化して認証情報蓄積サーバに登録するとともにその暗号化および復号化のための鍵情報、登録端末機種情報、ユーザID情報を搬送可能な個人情報蓄積媒体に記録しておき、認証端末において認証を受ける際に、上記した認証情報蓄積サーバから取得した暗号済みのバイオメトリク

ス情報をその個人情報蓄積媒体の暗号化鍵を用いて復号し、復号化したバイオメトリクス情報と、改めて入力したバイオメトリクス情報とを照合することでユーザの認証をおこなうことを特徴としている。

【0025】図1は、実施の形態1にかかる認証システムの概略構成を示すブロック図である。図1において、実施の形態1にかかる認証システムは、認証情報蓄積サーバ10と、登録端末20と、認証端末40とを備えて構成され、これらは通信回線9を介して通信可能に接続されている。

【0026】認証情報蓄積サーバ10は、インターネット上のWebサーバと同様な構成であり、いわゆる一般的なコンピュータシステムである。但し、ここで、認証情報蓄積サーバ10は、登録端末20から送信された個人認証情報を登録して蓄積するとともに、認証端末40からの要求に応じて、蓄積された個人認証情報を返信する。

【0027】登録端末20は、通信回線9を介して提供される電子商取引等の種々のサービスを受けることができるデスクトップコンピュータ、ノートコンピュータ、PDA(Personal Digital Assistant)、携帯電話等と同様な装置構成に、バイオメトリクス情報を入力することが可能な個人認証情報入力部22と、個人情報蓄積媒体30とを設けて構成される。

【0028】認証端末40は、登録端末20の個人認証情報入力部22と同構成の個人認証情報入力部42と、個人情報蓄積媒体30とを設けて構成され、全体の構成は登録端末20と変わらない。よって、登録端末20と認証端末40とは装置構成上特に区別されないが、少なくとも双方において、個人認証情報入力部22および42と個人情報蓄積媒体30を装填可能なスロットとはそれぞれ共通の仕様である必要がある。

【0029】例えば、個人認証情報入力部22および42は、バイオメトリクス情報としてユーザの指紋を入力する場合には、指紋スキャナであり、バイオメトリクス情報としてユーザの筆跡を入力する場合にはスタイラスペンを用いて入力可能なタブレットのような入力パッドである。

【0030】また、個人情報蓄積媒体30は、携帯が容易な不揮発性記憶媒体であり、例えば、磁気カード、フラッシュメモリカード、ICカードなどである。よって、登録端末20には、この個人情報蓄積媒体30を装填することが可能なスロットが設けられている。

【0031】また、通信回線9は、有線か無線かを問わず、公衆の電話回線網でも専用回線であってもよい。また、それら通信回線上に構築されたインターネット等のIP網をも含む。

【0032】以下に、実施の形態1にかかる認証システムの動作について説明する。図2は、実施の形態1にかかる認証システムの動作を示すフローチャートである。

図2において、まず、ユーザは、登録端末20の個人認証情報入力部22を介して、その個人認証情報入力部22において入力可能な自己のバイオメトリクス情報を入力する(ステップS101)。例えば、個人認証情報入力部22が指紋スキャナである場合には、登録端末20は、指紋スキャナで読み取った指紋画像から特徴点照合法に基づく特徴点を抽出し、抽出した特徴点の情報をバイオメトリクス情報として取得する。

【0033】つぎに、登録端末20は、取得したバイオメトリクス情報に対して、所定の暗号化鍵e1により暗号処理を施す(ステップS102)。なお、この暗号化鍵e1は、ユーザID情報や登録端末20の機種情報等とともに、個人情報蓄積媒体30に記録されている。

【0034】つづいて、登録端末20は、暗号化されたバイオメトリクス情報を、上記したユーザID情報や登録端末20の機種情報等とともに、通信回線9を介して認証情報蓄積サーバ10に送信する(ステップS103)。認証情報蓄積サーバ10は、暗号化済みのバイオメトリクス情報等の登録情報を受け取ると、個人認証情報データベース12に、その登録情報を登録する(ステップS201)。

【0035】ユーザは、以上のような手順によってバイオメトリクス情報の登録処理を終えると、登録端末20に装填していた個人情報蓄積媒体30を取り外し、認証端末40において認証処理が必要な場合以外は携帯等により厳重に保管しておく。特に、個人情報蓄積媒体30は、利用制限された建造物の入退出時や電子マネーの利用時などの他の認証をおこなうIDカードとしての機能を兼用させてもよく、この場合、ユーザは、複数の記録媒体を携帯する必要がなく、利用時の混乱も生じなくなる。

【0036】つぎに、ユーザは、登録端末20とは異なる認証端末40を使用する際、その認証端末40に個人情報蓄積媒体30を装填する。そして、ユーザは、認証端末40自体を使用する際に、または、認証端末40によって通信回線9を介したサービスを受ける際に要求されるユーザ認証に対して、登録端末20を用いたバイオメトリクス情報の入力手順と同様に、認証端末40の個人認証情報入力部42を介して、自己のバイオメトリクス情報を入力する(ステップS301)。

【0037】認証端末40は、ユーザによって入力されたバイオメトリクス情報を一端保持し、認証情報蓄積サーバ10に向けて、登録済みの個人認証情報、すなわち暗号化済みのバイオメトリクス情報の要求を、個人情報蓄積媒体30に記録されたユーザID情報や登録端末20の機種情報等とともに発信する(ステップS302)。

【0038】認証情報蓄積サーバ10は、認証端末40から上記個人認証情報要求を受け取ると、その個人認証情報要求に含まれるユーザID情報や登録端末20の機

種情報等に応じた暗号済みのバイオメトリクス情報を、個人認証情報データベース12から取り出し、認証端末40に返信する(ステップS202)。

【0039】認証端末40は、認証情報蓄積サーバ10から暗号済みのバイオメトリクス情報を受け取ると、その暗号済みのバイオメトリクス情報を、個人情報蓄積媒体30に記録された暗号化鍵e1を用いて復号化する

(ステップS303)。そして、認証端末40は、この復号化で得られたバイオメトリクス情報と、上記ステップS301において入力されたバイオメトリクス情報とを照合し、両者が一致しているかを判断する(ステップS304)。

【0040】認証端末40は、両者が一致していると判断すると、認証端末40自体の使用や通信回線9を介したサービスの享受が可能な状態に移行し、その旨のメッセージ等を表示する。逆に、両者が一致していない場合には、バイオメトリクス情報の再入力促すメッセージや警告等を表示する。

【0041】以上に説明したとおり、実施の形態1にかかる認証システムによれば、あらかじめ登録したバイオメトリクス情報を、外部に位置する認証情報蓄積サーバ10が管理するので、登録端末20と認証端末40のように、ユーザが登録時とは異なる端末を利用しようとする場合でも容易に個人認証を実行することが可能となる。

【0042】また、異なる端末間において利用可能な個人情報蓄積媒体30に暗号化鍵e1を記録しているので、その暗号化鍵e1で暗号化されたバイオメトリクス情報を、個人情報蓄積媒体30を介して復号化することができ、結果的に、認証情報蓄積サーバ10上に、バイオメトリクス情報を暗号化した状態で蓄積しておくことができる。換言すると、個人情報蓄積媒体30を装填していない端末では、ユーザ認証が不可能であり、高い安全性が確保される。

【0043】また、上記個人情報蓄積媒体30には少なくとも暗号/復号のための鍵情報のみを保持すればよいので、バイオメトリクス情報のサイズが大きい場合でも、個人情報蓄積媒体30の記憶量を圧迫することはない。例えば、バイオメトリクス情報が指紋情報の場合、複数の認証端末間において異なる指紋スキャナが備えられている場合であっても、登録端末20の指紋スキャナと認証端末40の指紋スキャナの仕様が一致さえしていれば、ユーザー一人に対して、複数の異なる仕様の指紋スキャナごとの指紋情報を登録することで、それぞれ個人認証が可能となる。

【0044】また、これは、ユーザー一人に対して、同じ種類のバイオメトリクス情報だけでなく異なる種類のバイオメトリクス情報を登録して利用できることを意味する。例えば、認証情報蓄積サーバ10に、一人のユーザに対して、指紋情報と筆跡情報の双方を暗号化した状態

で登録し、指紋スキャナを備えた認証端末と入力パッドを備えた認証端末の双方においてユーザ認証をおこなうことが可能である。すなわち、登録端末の機種情報を用いることで複数の異なる認証用機構を使い分けることができる。

【0045】実施の形態2. つぎに、実施の形態2にかかる認証システムについて説明する。実施の形態2にかかる認証システムは、電子商取引サービスの提供等をおこなうアプリケーションサーバからユーザ認証が求められた場合に、アプリケーションサーバによって公開鍵で暗号化されたセッションキーを受け取り、秘密鍵で復号化してそのセッションキーを取り出すとともに、取り出したセッションキーと実施の形態1にかかる認証システムによって照合された照合結果とをさらに秘密鍵で暗号化してアプリケーションサーバに返送することで、アプリケーションサーバにおいてより信頼性の高いユーザ認証を可能としたことを特徴としている。

【0046】図3は、実施の形態2にかかる認証システムの概略構成を示すブロック図である。なお、図3において、図1と共通する部分には同一の符号を付してその説明を省略する。図3に示す認証システムでは、登録端末20および認証端末40に装填される個人情報蓄積媒体30に、暗号化鍵e1に加えて、秘密鍵Es1の情報が記録されている点と、アプリケーションサーバ50を備えている点が、図1と異なる。

【0047】ここで、アプリケーションサーバ50は、通信回線9と接続されて電子商取引等の種々のサービスを提供するとともに、上記秘密鍵Es1と対になる公開鍵を入手しており、ユーザ認証の手順として、認証端末40に対するセッションキーKs1の発行をおこなう。なお、具体的な装置構成は、認証情報蓄積サーバ10と同様のコンピュータシステムである。

【0048】以下に、実施の形態2にかかる認証システムの動作について説明する。図4は、実施の形態2にかかる認証システムの動作を示すフローチャートである。なお、実施の形態2にかかる認証システムの動作において、図2に示したステップS101～S103、S201、S202、S301～S304の各処理は共通するため、ここでは特にそれらの説明を省略する。特に、図4では、説明を簡単にするため、図2に示したステップS101～S103、S201の図示を省略している。

【0049】よって、ここでは、認証端末40による照合処理(ステップS304)の後の動作について説明する。認証端末40における照合処理が終わった後、ユーザが、アプリケーションサーバ50が提供するサービスを享受したいとして、そのアプリケーションサーバ50にアクセスしたとすると、アプリケーションサーバ50は、このアクセスに対して、まず、セッションキーを乱数生成する。つづいて、アプリケーションサーバ50は、生成したセッションキーを、あらかじめ入手してい

た公開鍵E p 1で暗号化した後（ステップS 4 0 1）、認証端末4 0に向けて送信する（ステップS 4 0 2）。ここで、アプリケーションサーバ5 0が入手している公開鍵E p 1は、そのアプリケーションサーバ5 0によるサービスを利用しようとしているユーザ固有の鍵であり、そのユーザが保持している秘密鍵E s 1と対になるものである。

【0 0 5 0】アプリケーションサーバ5 0による公開鍵E p 1の入手は、例えば、ユーザが初めてそのアプリケーションサーバ5 0にアクセスした際に、アプリケーションサーバ5 0からユーザに対して公開鍵E p 1を送信する旨の指示を与えることによって実現される。なお、ユーザは、そのユーザ固有の公開鍵E p 1および秘密鍵E s 1の鍵ペアを、第三者信用機関である認証局から取得してもよいし、認証情報蓄積サーバ1 0が発行することにより取得してもよく、特に限定しない。

【0 0 5 1】認証端末4 0は、アプリケーションサーバ5 0から暗号済みのセッションキーを受け取ると、個人情報蓄積媒体3 0に記録された秘密鍵E s 1を用いてセッションキーを復号化する（ステップS 3 0 5）。さらに、認証端末4 0は、ステップS 3 0 4においておこなわれた照合の結果を示すメッセージとステップS 3 0 5において復号化されたセッションキーとを秘密鍵E s 1を用いて暗号化し（ステップS 3 0 6）、アプリケーションサーバ5 0に送信する（ステップS 3 0 7）。

【0 0 5 2】アプリケーションサーバ5 0は、認証端末4 0から、暗号化された照合結果およびセッションキーを受け取ると、公開鍵E p 1を用いて復号化し、復号化された照合結果が一致を示し、かつ復号されたセッションキーがステップS 4 0 2において認証端末4 0に送信したものと一致しているか否かを照合する（ステップS 4 0 3）。一致している場合には、正当なユーザからのアクセスであると判断され、アプリケーションサーバ5 0は、上記セッションキーまたは新たに発行したセッションキーと、秘密鍵および公開鍵とを用いた、いわゆる共通鍵暗号法と公開鍵暗号法とを組み合わせた暗号通信により、サービスの提供をおこなう。

【0 0 5 3】このように、アプリケーションサーバ5 0が認証端末4 0に対してサービスを提供する際には、通常、そのセキュリティを向上させるためにセッションキーの発行をおこなっており、本実施の形態では、そのセッションキーを、ユーザ認証をおこなうために利用している。

【0 0 5 4】以上に説明したとおり、実施の形態2にかかる認証システムによれば、実施の形態1にかかる認証システムの構成に対して、個人情報蓄積媒体3 0にさらに秘密鍵E s 1の情報を記録し、アプリケーションサーバ5 0が発行するセッションキーと認証端末4 0上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りすることで、アプリケーションサーバ5 0

側が要求するユーザ認証をも可能にするので、実施の形態1による効果に加え、アプリケーションサーバ5 0側から見て、信頼度の高いユーザ認証をおこなうことができる。

【0 0 5 5】実施の形態3. つぎに、実施の形態3にかかる認証システムについて説明する。実施の形態3にかかる認証システムは、実施の形態1において示した認証情報蓄積サーバを複数設置し、なおかつ各認証情報蓄積サーバは同内容の個人認証情報データベースを備えていることを特徴としている。

【0 0 5 6】図5は、実施の形態3にかかる認証システムの概略構成を示すブロック図である。なお、図5において、図1と共通する部分には同一の符号を付してその説明を省略する。図5に示す認証システムでは、複数の認証情報蓄積サーバ1 0-1～1 0-nを備えている点が、図1と異なる。

【0 0 5 7】特に、各認証情報蓄積サーバが備えている個人認証情報データベース1 2は、同内容であり、登録端末2 0および認証端末4 0は、いずれの認証情報蓄積サーバに対しても、登録処理またはバイオメトリクス情報取得処理をおこなうことができる。

【0 0 5 8】例えば、登録端末2 0が、認証情報蓄積サーバ1 0-1に対し、実施の形態1において説明したようにバイオメトリクス情報の登録処理をおこなった場合には、認証情報蓄積サーバ1 0-1は、個人認証情報データベース1 2において登録処理により変更のあった部分を、他の認証情報蓄積サーバ1 0-2～1 0-nに通知し、認証情報蓄積サーバ1 0-2～1 0-nは、それぞれその通知に従って自己が備える個人認証情報データベース1 2の内容を更新する。

【0 0 5 9】すなわち、認証情報蓄積サーバ1 0-1～1 0-nは、互いにミラーサーバの関係にあり、常に、同一の内容のバイオメトリクス情報を保持する。よって、認証端末4 0は、いずれの認証情報蓄積サーバにアクセスしたとしても、最新のバイオメトリクス情報を取得することができる。なお、認証端末4 0において、通信経路の最も短い位置にある認証情報蓄積サーバをあらかじめ登録しておき、通常利用時にはその認証情報蓄積サーバを利用するようにしてもよい。この際、その通常利用時の認証情報蓄積サーバが、何らかの障害によってダウンした場合には、自動的に、他の認証情報蓄積サーバに切り替わるように設定しておくことができる。

【0 0 6 0】以上に説明したとおり、実施の形態3にかかる認証システムによれば、複数の認証情報蓄積サーバ1 0-1～1 0-nにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができ、確実な認証が可能となる。また、特に、応答速度の速い認証情報蓄積サーバを通常利用時のサーバに設定しておくことで、ネットワークトラフィックの状況によらず、迅速な認証

が可能となり、認証要求を出した端末と登録端末が地理的に異なる地点であっても、その影響を受けない認証が可能である。

【0061】実施の形態4. つぎに、実施の形態4にかかる認証システムについて説明する。実施の形態4にかかる認証システムは、登録端末を用いて入力したバイオメトリクス情報を複数の情報に分割し、分割した各情報を暗号化して複数の認証情報蓄積サーバに分散して蓄積し、その暗号化および復号化のための鍵情報、登録端末機種情報、ユーザID情報、分散した認証情報蓄積サーバの情報を搬送可能な個人情報蓄積媒体に記録することを特徴としている。

【0062】図6は、実施の形態4にかかる認証システムの概略構成を示すブロック図である。図6において、実施の形態4にかかる認証システムは、第1の認証情報蓄積サーバ100(1)～第nの認証情報蓄積サーバ100(n)と、登録端末120と、認証端末140とを備えて構成され、これらは通信回線9を介して通信可能に接続されている。

【0063】第1の認証情報蓄積サーバ100(1)～第nの認証情報蓄積サーバ100(n)は、実施の形態1で説明した認証情報蓄積サーバ10と同様な構成である。但し、第1の認証情報蓄積サーバ100(1)～第nの認証情報蓄積サーバ100(n)の各認証情報蓄積サーバにおいて蓄積されるバイオメトリクス情報は、互いに異なっている。

【0064】登録端末120は、実施の形態1で説明した登録端末20と同様な構成であり、個人認証情報入力部122と、個人情報蓄積媒体30とを設けているが、それらに加えてさらに認証情報分割部124を備えている。認証情報分割部124は、個人認証情報入力部122を介して入力されたバイオメトリクス情報を複数の情報に分割する手段である。例えば、個人認証情報入力部122によって指紋画像が読み込まれたとすると、その指紋画像から特徴点照合法に基づく特徴点を抽出するとともに、抽出した特徴点の情報をさらに、端点や分岐点等の種類、位置、隆線間隔別の情報に分割する。

【0065】認証端末140は、実施の形態1で説明した認証端末40と同様な構成であり、個人認証情報入力部142と、個人情報蓄積媒体30とを設けているが、それらに加えてさらに認証情報併合部144を備えている。認証情報併合部144は、登録端末120の認証情報分割部124によって分割されたバイオメトリクス情報を元の一つのバイオメトリクス情報に復元する手段である。

【0066】また、個人情報蓄積媒体30は、実施の形態1と同様に、携帯が容易な不揮発性記憶媒体であり、通信回線9は、実施の形態1と何ら変わらない。

【0067】以下に、実施の形態4にかかる認証システムの動作について説明する。図7は、実施の形態4にか

かる認証システムの動作を示すフローチャートである。図7において、まず、ユーザは、実施の形態1に説明したように、登録端末120の個人認証情報入力部122を介して、その個人認証情報入力部122において入力可能な自己のバイオメトリクス情報を入力する(ステップS111)。

【0068】つぎに、登録端末120は、取得したバイオメトリクス情報に対し、認証情報分割部124によって、所定の複数のバイオメトリクス情報に分割する(ステップS112)。特に、第1の認証情報蓄積サーバ100(1)～第nの認証情報蓄積サーバ100(n)がそれぞれ蓄積する情報の種別に対応するように分割される。

【0069】さらに、登録端末120は、複数の分割された各バイオメトリクス情報に対して、所定の暗号化鍵e1により暗号処理を施す(ステップS113)。なお、この暗号化鍵e1は、ユーザID情報や登録端末120の機種情報等とともに、個人情報蓄積媒体30に記録されている。ここで、分割された各バイオメトリクス情報に対して用いる暗号化鍵e1は、共通のものであってもよいし、各情報間で異なるものであってもよい。なお、この暗号化鍵e1は、ユーザID情報、登録端末120の機種情報および登録先である第1の認証情報蓄積サーバ100(1)～第nの認証情報蓄積サーバ100(n)の各サーバ情報等とともに、個人情報蓄積媒体30に記録されている。

【0070】つづいて、登録端末120は、暗号化された各バイオメトリクス情報を、上記したユーザID情報や登録端末120の機種情報等とともに、通信回線9を介して、個人情報蓄積媒体30に記録された上記サーバ情報に基づいて、第1の認証情報蓄積サーバ100

(1)～第nの認証情報蓄積サーバ100(n)に送信する(ステップS114)。第1の認証情報蓄積サーバ100(1)～第nの認証情報蓄積サーバ100(n)の各サーバは、暗号化済みのバイオメトリクス情報等の登録情報を受け取ると、個人認証情報データベース12に、その登録情報を登録する(ステップS211)。

【0071】ユーザは、以上のような手順によってバイオメトリクス情報の登録処理を終えると、登録端末120に装填していた個人情報蓄積媒体30を取り外し、実施の形態1において説明するように、認証端末140において認証処理が必要な場合以外は携帯等により厳重に保管しておく。

【0072】つぎに、ユーザは、認証端末140を使用する際、その認証端末140に個人情報蓄積媒体30を装填する。そして、ユーザは、認証端末140自体を使用する際に、または、認証端末140によって通信回線9を介したサービスを楽しむ際に要求されるユーザ認証に対して、登録端末120を用いたバイオメトリクス情報の入力手順と同様に、認証端末140の個人認証情

報入力部142を介して、自己のバイオメトリクス情報を入力する（ステップS311）。

【0073】認証端末140は、ユーザによって入力されたバイオメトリクス情報を一端保持し、個人情報蓄積媒体30に記録されたサーバ情報により決定される第1の認証情報蓄積サーバ100（1）～第nの認証情報蓄積サーバ100（n）に向けて、登録済みの個人認証情報、すなわち暗号化済みのバイオメトリクス情報の要求を、個人情報蓄積媒体30に記録されたユーザID情報や登録端末120の機種情報等とともに発信する（ステップS312）。

【0074】第1の認証情報蓄積サーバ100（1）～第nの認証情報蓄積サーバ100（n）の各サーバは、認証端末140から上記個人認証情報要求を受け取ると、その個人認証情報要求に含まれるユーザID情報や登録端末120の機種情報等に応じた暗号済みのバイオメトリクス情報を、個人認証情報データベース12から取り出し、認証端末140に返信する（ステップS212）。

【0075】認証端末140は、第1の認証情報蓄積サーバ100（1）～第nの認証情報蓄積サーバ100（n）の各サーバから暗号済みのバイオメトリクス情報を受け取ると、各暗号済みのバイオメトリクス情報を、それぞれ個人情報蓄積媒体30に記録された暗号化鍵e1を用いて復号化する（ステップS313）。さらに、認証端末140は、この復号化で得られた各バイオメトリクス情報を、認証情報併合部144によって、元の一つのバイオメトリクス情報に併合して復元する（ステップS314）。

【0076】そして、認証端末140は、この併合によって得られたバイオメトリクス情報と、上記ステップS311において入力されたバイオメトリクス情報とを照合し、両者が一致しているかを判断する（ステップS315）。

【0077】認証端末140は、両者が一致していると判断すると、認証端末140自体の使用や通信回線9を介したサービスの享受が可能な状態に移行し、その旨のメッセージ等を表示する。逆に、両者が一致していない場合には、バイオメトリクス情報の再入力を促すメッセージや警告等を表示する。

【0078】以上に説明したとおり、実施の形態1にかかる認証システムによれば、実施の形態1による効果を楽しむことができるとともに、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなる。また、各認証情報蓄積サーバは分割されたバイオメトリクス情報を保持しているので、一つの認証情報蓄積サーバに蓄積されたバイオメトリクス情報のみではユーザ認証を受けることができず、高い安全性が確保され

る。

【0079】また、端末間で移動する個人情報蓄積媒体30には少なくとも分散先となる認証情報蓄積サーバと分割されたバイオメトリクス情報の種別とを含めたサーバ情報を保持すればよいので、バイオメトリクス情報のサイズが大きい場合でも、個人情報蓄積媒体30の記憶量を圧迫することない。

【0080】実施の形態5. つぎに、実施の形態5にかかる認証システムについて説明する。実施の形態5にかかる認証システムは、実施の形態2において示した認証情報蓄積サーバを、実施の形態3に示したように複数設置し、なおかつ各認証情報蓄積サーバは同内容の個人認証情報データベースを備えていることを特徴としている。

【0081】図8は、実施の形態5にかかる認証システムの概略構成を示すブロック図である。なお、図8において、図3と共通する部分には同一の符号を付してその説明を省略する。図8に示す認証システムでは、図5に示したように、複数の認証情報蓄積サーバ10-1～10-nを備えている点が、図3と異なる。

【0082】以上に説明したとおり、実施の形態5にかかる認証システムによれば、実施の形態2による効果を楽しむことができるとともに、複数の認証情報蓄積サーバ10-1～10-nにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができ、確実な認証が可能となる。また、特に、応答速度の速い認証情報蓄積サーバを通常利用時のサーバに設定しておくことで、ネットワークトラフィックの状況によらず、迅速な認証が可能となり、認証要求を出した端末と登録端末が地理的に異なる地点であっても、その影響を受けない認証が可能である。

【0083】実施の形態6. つぎに、実施の形態6にかかる認証システムについて説明する。実施の形態6にかかる認証システムは、実施の形態4において示した第1の認証情報蓄積サーバ～第nの認証情報蓄積サーバの各サーバを、さらに実施の形態3に示したように複数設置することを特徴としている。

【0084】図9は、実施の形態6にかかる認証システムの概略構成を示すブロック図である。なお、図9において、図5および図6と共通する部分には同一の符号を付してその説明を省略する。図9に示す認証システムでは、第1の認証情報蓄積サーバ10-1（1）～第mの認証情報蓄積サーバ10-1（m）の各サーバに対して、複数のミラーサーバを設置している点が、図6と異なる。例えば、第1の認証情報蓄積サーバ10-1（1）に対しては、同一のバイオメトリクス情報を蓄積した複数の第1の認証情報蓄積サーバ10-2（1）～10-n（1）が設置される。

【0085】以上に説明したとおり、実施の形態6にか

かる認証システムによれば、実施の形態4にかかる認証システムにおいて、分割されたバイオメトリクス情報を分散して蓄積する第1の認証情報蓄積サーバ10-1

(1)～第mの認証情報蓄積サーバ10-1(m)の各サーバについて、実施の形態3において示したように複数のミラーサーバを設けるので、実施の形態4による効果に加え、実施の形態3による効果を楽しむことができる。

【0086】なお、実施の形態6に示したように、分割されたバイオメトリクス情報を複数の認証情報蓄積サーバに分散させるとともに、各認証情報蓄積サーバに複数のミラーサーバを設置する構成は、実施の形態2にかかる認証システムに適用させることも可能であることは言うまでもない。

【0087】

【発明の効果】以上、説明したとおり、この発明によれば、あらかじめ登録したバイオメトリクス情報を、外部に位置する認証情報蓄積サーバが管理するので、認証端末のように、ユーザが登録時に使用した登録端末とは異なる端末を利用しようとする場合でも、個人情報蓄積媒体を移すことのみで、暗号化をともなった個人認証を実行することが可能となるとともに、個人情報蓄積媒体を装填していない端末では、ユーザ認証が不可能となり、高い安全性が確保されるという効果を奏する。

【0088】つぎの発明によれば、個人情報蓄積媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、アプリケーションサーバ側が要求するユーザ認証を高い信頼度で可能にするという効果を奏する。

【0089】つぎの発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなり、結果的に一つの認証情報蓄積サーバに蓄積されたバイオメトリクス情報のみではユーザ認証を受けることができず、高い安全性が確保されるという効果を奏する。

【0090】つぎの発明によれば、登録情報を複数の認証情報蓄積サーバに分散して登録しておき、認証時にはそれらのサーバからの情報を併合するとともに、個人情報

報告媒体に暗号化鍵および秘密鍵の情報を記録し、アプリケーションサーバが発行するセッションキーと認証端末上でのバイオメトリクス情報の照合結果とを公開鍵暗号法によってやり取りするので、一つのバイオメトリクス情報が一つのサーバで集中して管理されることがなくなり、高い安全性を確保することができるとともに、アプリケーションサーバ側が要求するユーザ認証を高い信頼度で可能にするという効果を奏する。

【0091】つぎの発明によれば、複数の認証情報蓄積サーバにバイオメトリクス情報を多重化して保持するので、一部のサーバがダウンしていても、他のサーバから情報を復号化することができ、確実な認証が可能となるという効果を奏する。

【図面の簡単な説明】

【図1】 実施の形態1にかかる認証システムの概略構成を示すブロック図である。

【図2】 実施の形態1にかかる認証システムの動作を示すフローチャートである。

【図3】 実施の形態2にかかる認証システムの概略構成を示すブロック図である。

【図4】 実施の形態2にかかる認証システムの動作を示すフローチャートである。

【図5】 実施の形態3にかかる認証システムの概略構成を示すブロック図である。

【図6】 実施の形態4にかかる認証システムの概略構成を示すブロック図である。

【図7】 実施の形態4にかかる認証システムの動作を示すフローチャートである。

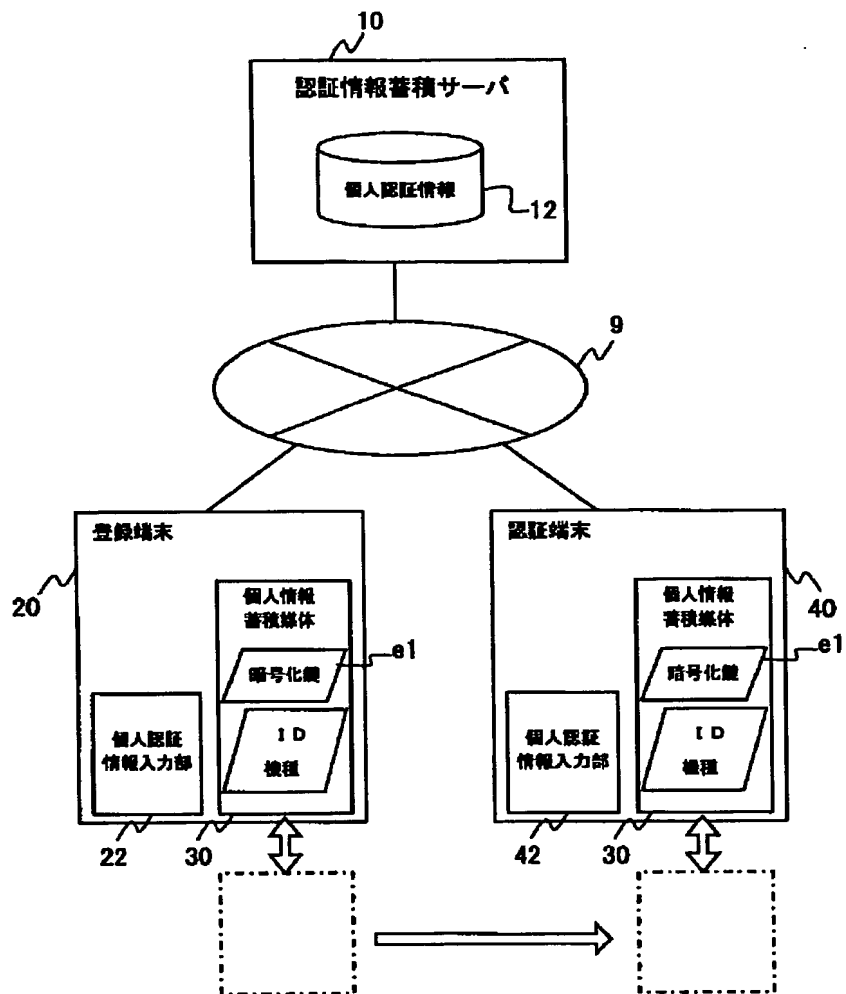
【図8】 実施の形態5にかかる認証システムの概略構成を示すブロック図である。

【図9】 実施の形態6にかかる認証システムの概略構成を示すブロック図である。

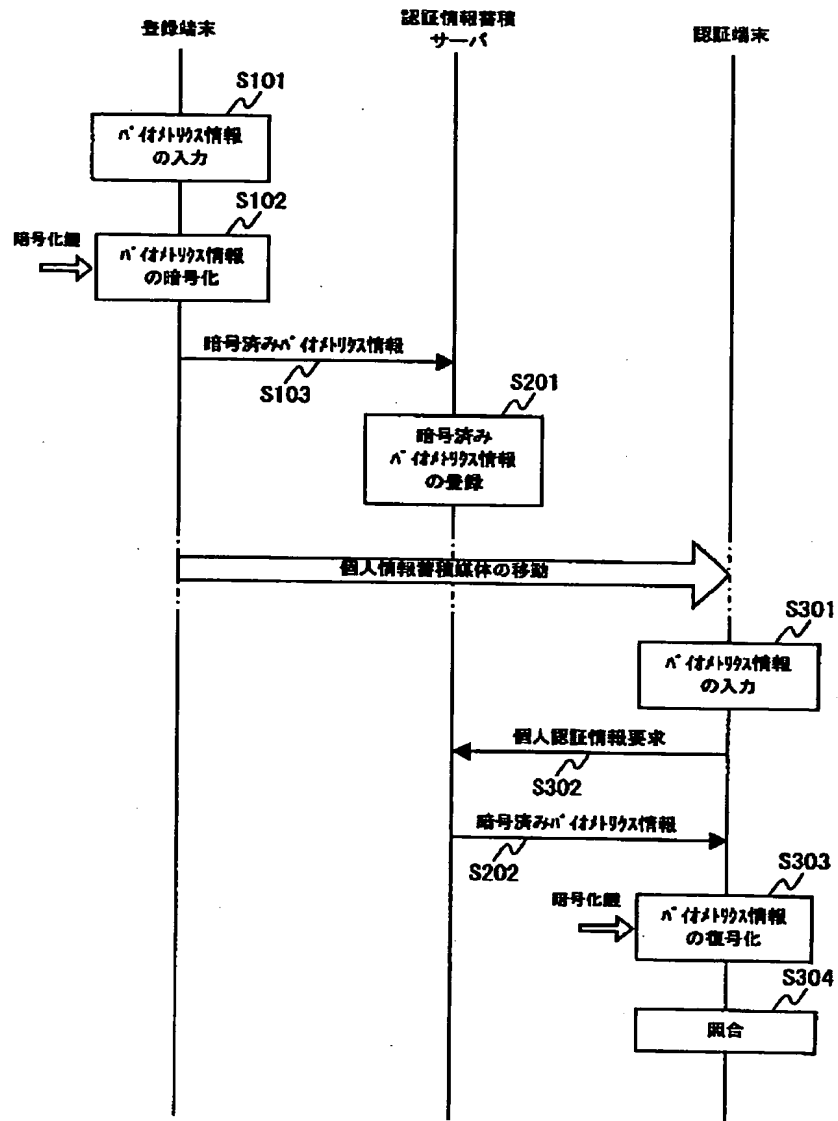
【符号の説明】

9 通信回線、10、100 認証情報蓄積サーバ、12 個人認証情報データベース、20、120 登録端末、22 個人認証情報入力部、22 個人認証情報入力部、30 個人情報蓄積媒体、40、140 認証端末、42、142 個人認証情報入力部、50 アプリケーションサーバ、100 認証情報蓄積サーバ、122 個人認証情報入力部、124 認証情報分割部、144 認証情報併合部。

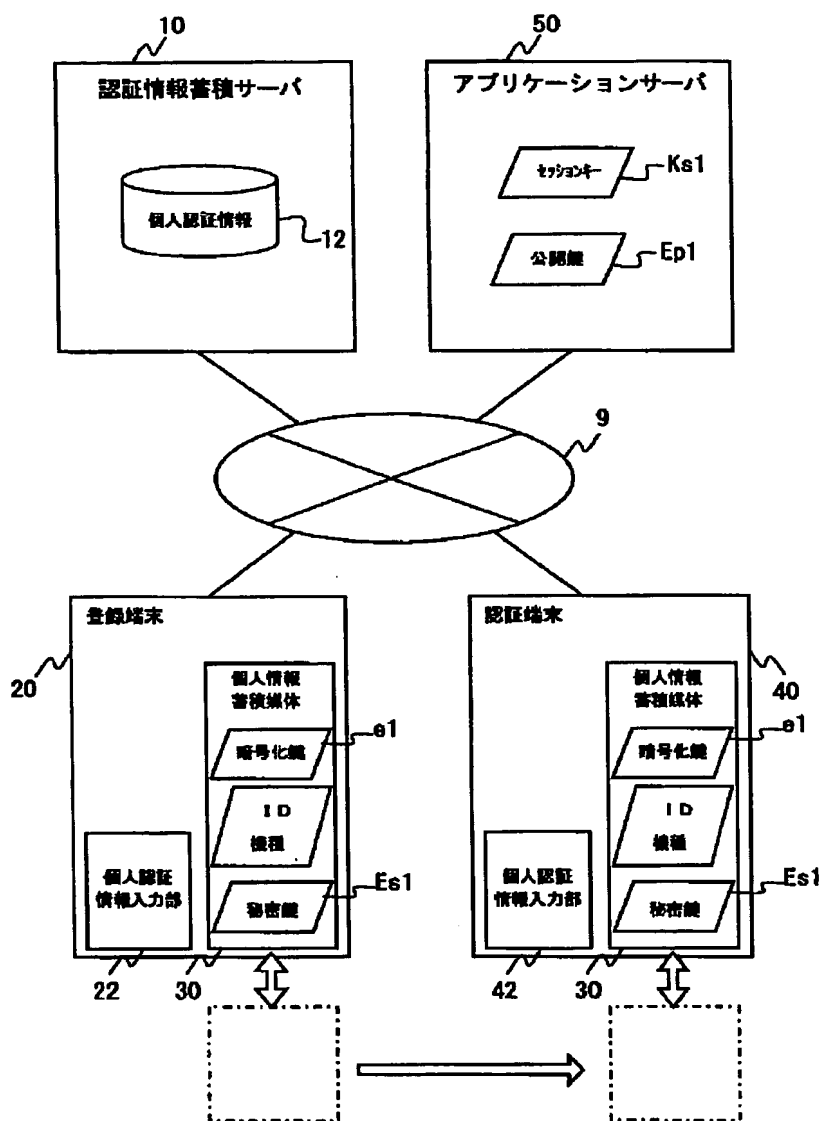
【図1】



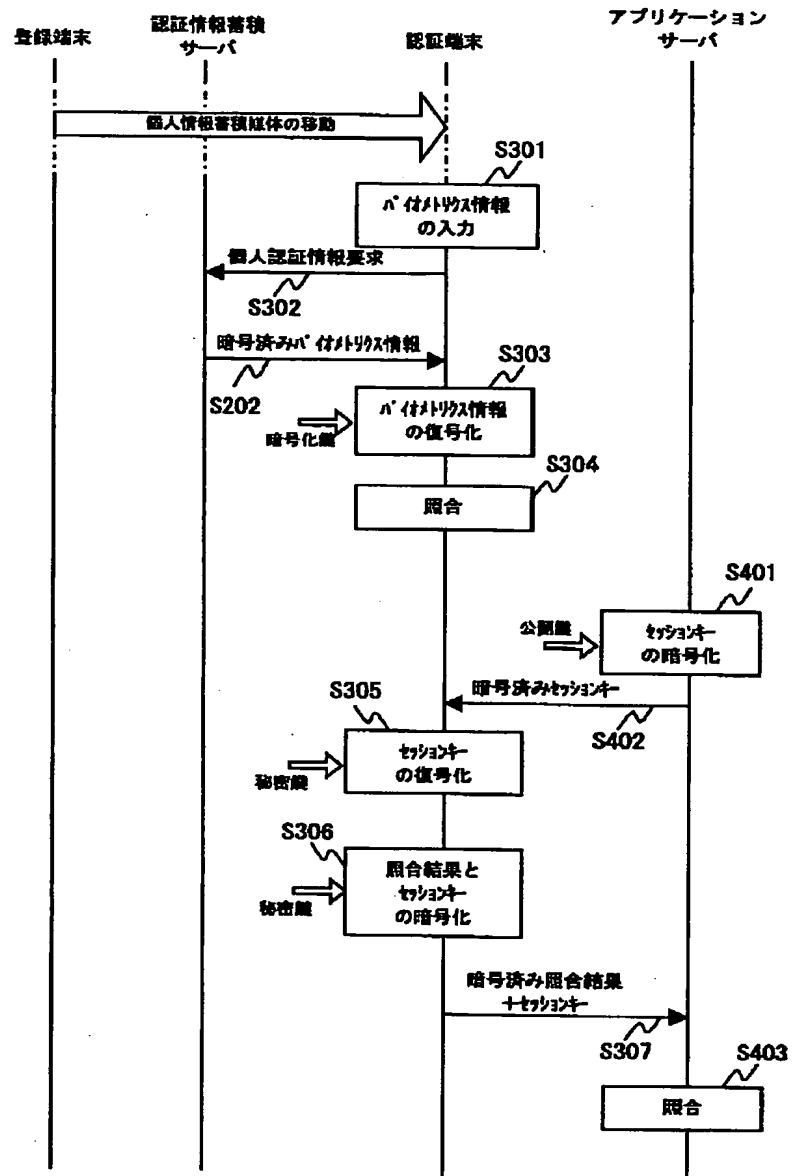
【図2】



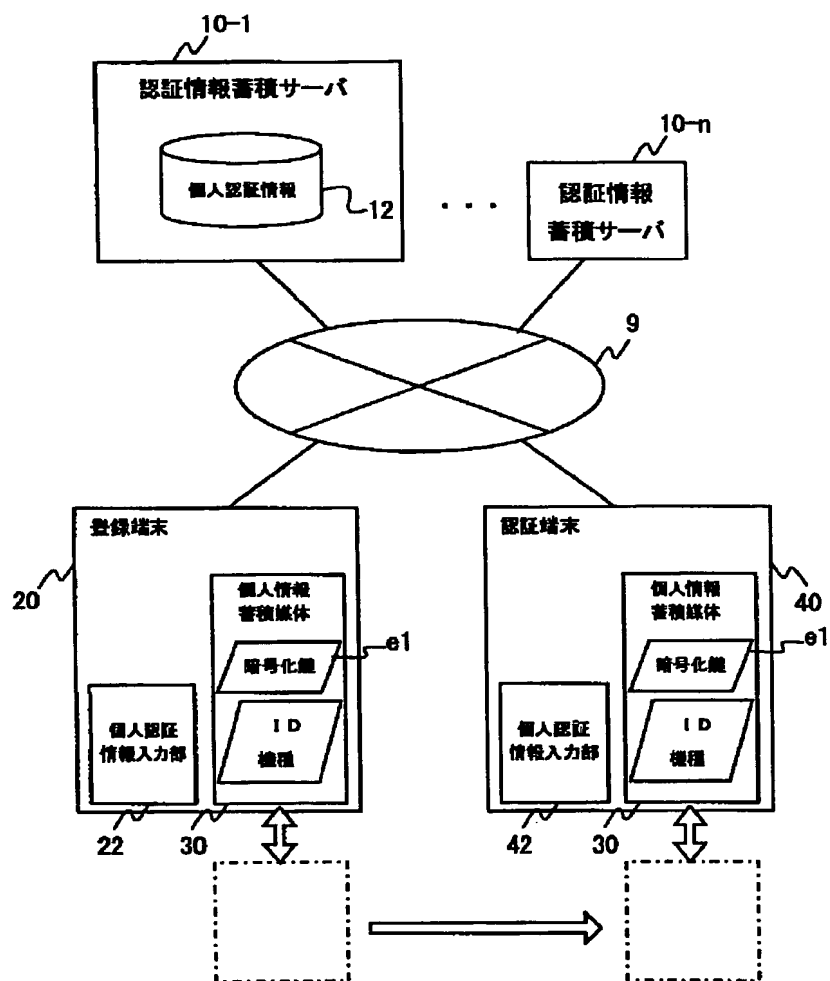
【図3】



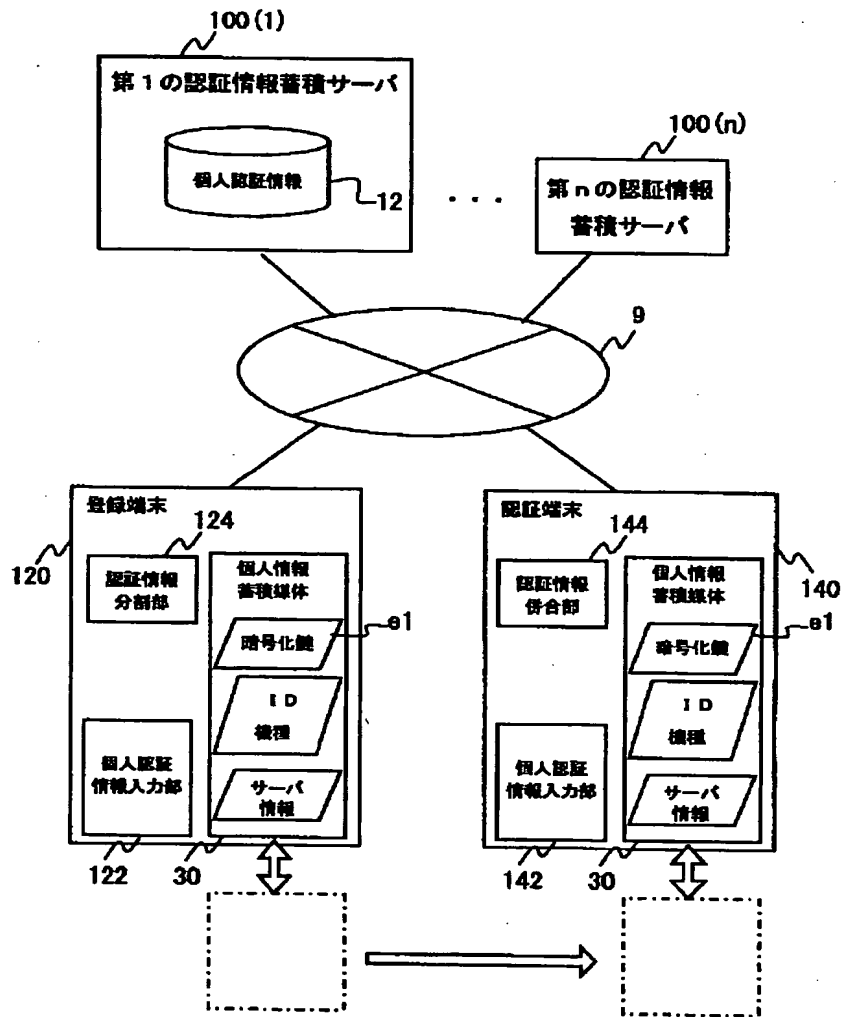
【図4】



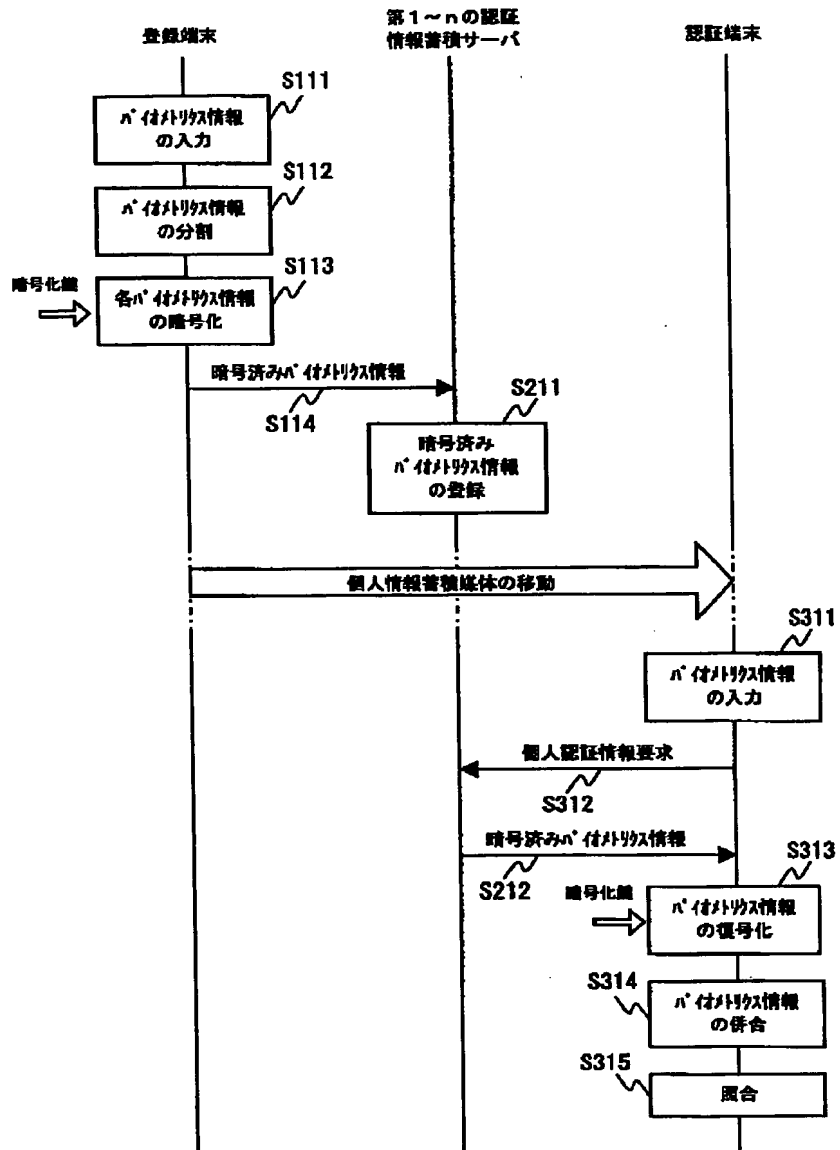
【図5】



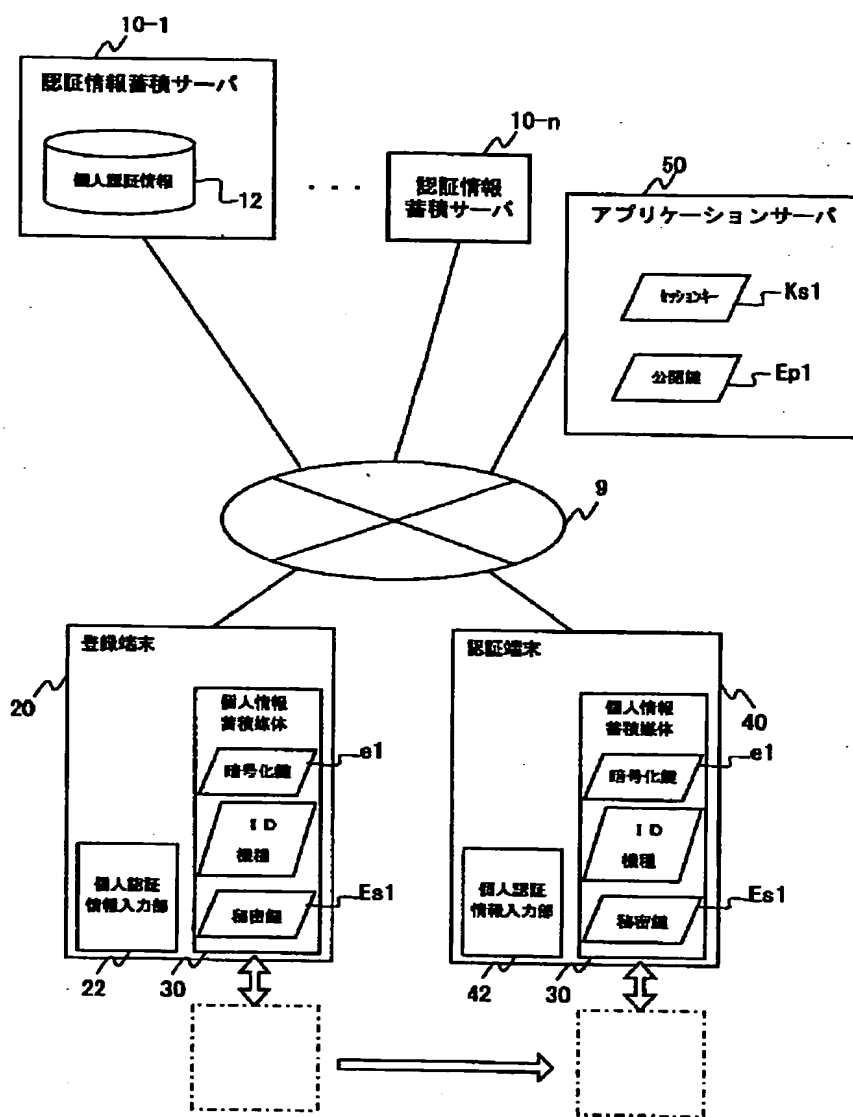
【図6】



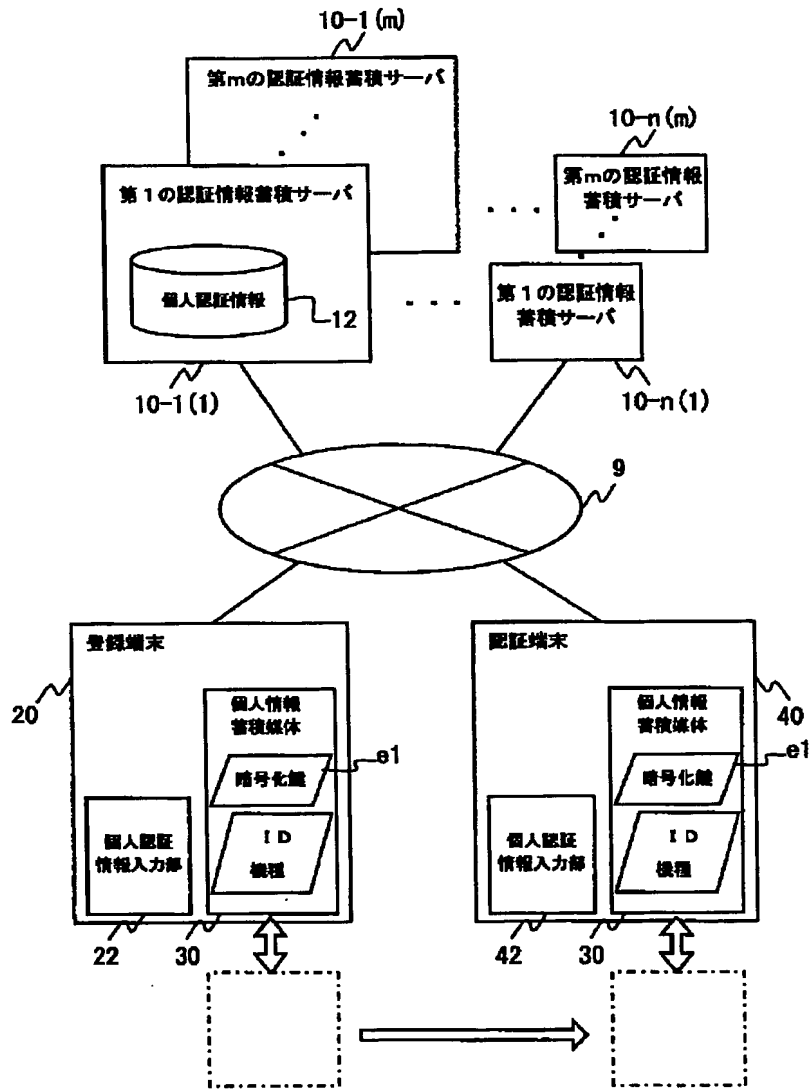
【図 7】



【図8】



【図9】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

H 0 4 L 9/00

テーマコード (参考)

6 7 5 D

(72)発明者 鹿井 正博
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 白附 晶英
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 岡 徹
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 田壺 宏和
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 篇田 広幸
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

Fターム(参考) 5B035 AA13 BB02 BB09 BC01
5B058 CA31 KA31 KA35 KA37 KA38
5B085 AA01 AE11 AE25 AE29
5J104 AA07 AA16 EA06 EA19 KA01
KA16 KA17 KA19 MA04 NA02
NA03 NA34 NA35 NA36 NA37
PA07 PA10

THIS PAGE BLANK (USPTO)